problems and interdependencies related to critical infrastructure and protected systems in order to ensure the availability, integrity, and reliability thereof;

(2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.

Local Government has the same meaning as is established in section 2 of the Homeland Security Act of 2002 and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in §29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

Protected System means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

Purpose of CII has the meaning set forth in section 214(a)(1) of the CII Act of 2002 and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

Submission to DHS as referenced in these procedures means any transmittal of CII to the DHS Protected CII Program Manager or the Protected CII Program Manager's designees, as set forth in §29.5.

Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (*i.e.*, come from) a single entity or by an ISAO acting on behalf of its members. In the case of any action brought under the securities laws—as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—the term "voluntary" does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanies the solicitation of an offer or a sale of securities. The term also explicitly excludes information or statements submitted during a regulatory proceeding or relied upon as a basis for making licensing or permitting determinations.

§29.3 Effect of provisions.

(a) *Mandatory submissions of information.* The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information

that must be submitted to DHS pursuant to a Federal legal requirement, nor do they pertain to any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted to DHS pursuant to the CII Act of 2002). The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information to a Federal agency under any other provision of law. Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002.

(b) *Freedom of Information Act disclosure exemptions.* Information that is separately exempt from disclosure under the Freedom of Information Act or applicable State or local law does not lose its separate exemption protection due to the applicability of these procedures or any failure to follow them.

(c) *Restriction on use of Protected CII by regulatory and other Federal agencies.* No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of that same information. Federal agencies shall not utilize Protected CII for regulatory purposes without the written consent of the submitter or another party on the submitter's behalf.

(d) *Independently obtained information.* These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local government entity, agency, or authority, or any third party, under applicable law, to otherwise obtain CII by means of a different law, regulation, rule, or other authority, including such information as is lawfully and customarily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.

(e) *No private right of action.* Nothing contained in these procedures is intended to confer any substantive or procedural right or privilege on any person or entity. Nothing in these procedures shall be construed to create a private right of action for enforcement of any provision of these procedures or a defense to noncompliance with any independently applicable legal obligation.

§ 29.4 Protected Critical Infrastructure Information Program administration.

(a) *IAIP Directorate Program Management.* The Secretary of the Department of Homeland Security hereby designates the Under Secretary of the Information Analysis and Infrastructure Protection (IAIP) Directorate as the senior DHS official responsible for the direction and administration of the Protected CII Program.

(b) *Appointment of a Protected CII Program Manager.* The Under Secretary for IAIP shall:

(1) Appoint a Protected CII Program Manager within the IAIP Directorate who is responsible to the Under Secretary for the administration of the Protected CII Program;

(2) Commit resources necessary to the effective implementation of the Protected CII Program;

(3) Ensure that sufficient personnel, including such detailees or assignees from other Federal national security, homeland security, or law enforcement entities as the Under Secretary deems appropriate, are assigned to the Protected CII Program to facilitate the expeditious and secure sharing with appropriate authorities, including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to